UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

JESSICA FLAGELLA, ON BEHALF OF HERSELF AND HER MINOR CHILDREN A.F. AND A.F., and all others similarly situated, Plaintiffs, v. **DOLLAR ENERGY FUND,** Defendant.	Case No. 2:23-cv-1988 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jessica Flagella, on behalf of herself and her minor children A.F. and A.F., ("Plaintiffs"), individually and on behalf of all similarly situated persons, alleges the following against Dollar Energy Fund ("DEF" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against DEF for its failure to properly secure and safeguard Plaintiffs' and other similarly situated DEF customers' names and social security numbers (the "Private Information") from hackers.

2. DEF, based in Pittsburgh, is a non-profit utility assistance service that serves tens of thousands of customers in 16 states across the United States.

3. On or about October 19, 2023, DEF filed official notice of a hacking incident with the Maine Attorney General's office. Under state law, organizations must report breaches involving Social Security numbers.

4. Based on the Notice filed by the company, on February 5th, 2023, DEF detected unusual activity on some of its computer systems. In response, the company launched an investigation. The DEF investigation revealed that an unauthorized party had access to certain company files between January 1, 2023, and February 5, 2023, (the "Data Breach"). Yet, DEF waited almost *six months* to notify the public that they were at risk.

5. As a result of this delayed response, Plaintiffs and "Class Members" (defined below) had no idea for almost six months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

6. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, names in connection with social security numbers that DEF collected and maintained.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by DEF that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs bring this class action lawsuit to address DEF's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

11. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to DEF, and thus DEF was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

12. Upon information and belief, DEF and its employees failed to properly monitor or to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had DEF properly monitored its networks, it would have discovered the Breach sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of DEF's negligent conduct as the Private Information that DEF collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for Negligence, Negligence Per Se, Breach of Contract, Breach of Implied Contract, Intrusion Upon Seclusion/Invasion of Privacy, Unjust Enrichment, and Declaratory Judgement.

II. PARTIES

16. Plaintiff Jessica Flagella, on behalf of her minor Children AF and AF, is, and at all times mentioned herein was, an individual citizen of the State of Pennsylvania.

17. Defendant Dollar Energy Fund is a non-profit organization organized under the laws of Pennsylvania, with its principal place of business at 15 Terminal Way, Pittsburgh, Pennsylvania in Allegheny County.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from DEF. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over DEF because DEF operates in and/or is incorporated in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and DEF has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. DEF's Business and Collection of Plaintiffs' and Class Members' Private Information

21. DEF is an energy corporation that provides utility assistance grants to families and individuals. As a condition of receiving utility assistance services, DEF requires that its customers entrust it with highly sensitive personal information.

22. In the ordinary course of receiving service from DEF, Plaintiff was required to provide her (and her minor children's) Private Information to Defendant.

23. In its privacy policy, DEF promises its customers that it will not share this Private Information with third parties: "We do not trade, share, sell, rent or otherwise provide personal information of donors to third parties."[1]

24. Because of the highly sensitive and personal nature of the information DEF acquires and stores with respect to its customers, DEF, upon information and belief, promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, DEF assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

[1] https://www.dollarenergy.org/privacy-policy/ (last visited on November 15, 2023).

26. Plaintiffs and Class Members relied on DEF to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. The Data Breach and DEF's Inadequate Notice to Plaintiffs and Class Members

27. According to Defendant's Notice, it learned of unauthorized access to its computer systems on February 5, 2023, with such unauthorized access having taken place between January 31, 2023 and February 5, 2023.

28. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names in connection with Social Security numbers.

29. On or about October 4, 2023, roughly six months after DEF learned that the Class's Private Information was first accessed by cybercriminals, DEF finally began to notify customers that its investigation determined that their Private Information was breached.

30. DEF delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "Cybersecurity incident."

31. DEF had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

32. Plaintiffs and Class Members provided their Private Information to DEF with the reasonable expectation and mutual understanding that DEF would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

33. DEF's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

34. DEF knew or should have known that its electronic records would be targeted by cybercriminals.

C. DEF Failed to Comply with FTC Guidelines

35. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

36. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

37. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. As evidenced by the Data Breach, DEF failed to properly implement basic data security practices. DEF's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

40. DEF was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. DEF Failed to Comply with Industry Standards

41. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

42. Some industry best practices that should be implemented by businesses like DEF include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

43. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports;

protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

44. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

45. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. DEF Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

46. In addition to its obligations under federal and state laws, DEF owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. DEF owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

47. DEF breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems

and data. DEF's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

48. DEF negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

49. Had DEF remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

50. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of

future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with DEF.

F. DEF Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

51. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

52. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

53. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on November 13, 2023).

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

54. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

55. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

56. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

57. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud,

[3] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited November 13, 2023).

to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

58. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

59. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[4] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

60. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can

[4] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on November 13, 2023).

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on November 13, 2023).

sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[6]

61. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[7]

62. The Dark Web Price Index of 2022, published by PrivacyAffairs[8] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

63. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

---

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on November 13, 2023).

[7] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on November 13, 2023).

[8] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on November 13, 2023).

64. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including DEF collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[9]

65. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[10]

66. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

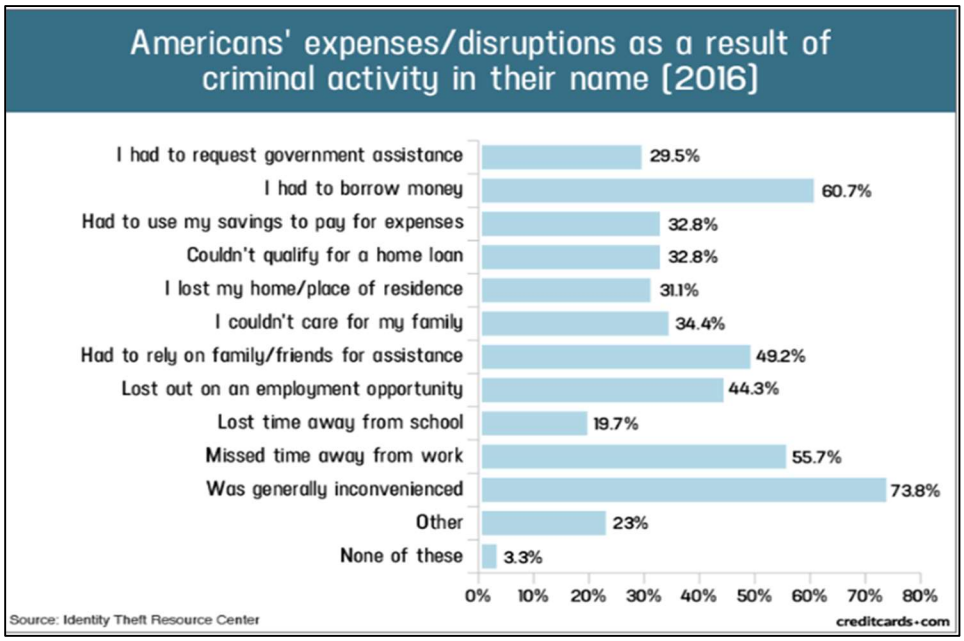
67. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

68. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

[9] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on November 13, 2023).

[10] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

69. A study by the Identity Theft Resource Center[11] shows the multitude of harms caused by fraudulent use of PII:



70. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[12]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[11] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited November 13, 2023).

[12] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited November 13, 2023).

71. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

72. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiffs' and Class Members' Damages

Plaintiff Flagella's Experience

73. When Plaintiff Flagella and her children became recipients of DEF's services, DEF required that she provide it with substantial amounts of her and her minor children's PII.

74. On or about October 4, 2023, Plaintiff Flagella received a letter which told her that her children's Private Information may have been accessed during the Data Breach. The notice letter informed her that the Private Information stolen included their full names and social security numbers. Upon information and belief, Plaintiff Flagella's Private Information was also accessed and/or acquired in the Data Breach.

75. Plaintiff Flagella suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

76. Plaintiff Flagella would not have provided her children's Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

77. Plaintiff Flagella and her minor children suffered actual injury in the form of having their Private Information compromised and/or stolen as a result of the Data Breach.

78. Plaintiff Flagella and her minor children also suffered actual injury in the form of damages to and diminution in the value of their Private Information – a form of intangible property that Plaintiff Flagella entrusted to Defendant for the purpose of receiving utility assistance services and which was compromised in, and as a result of, the Data Breach.

79. Plaintiff Flagella and her minor children also suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being placed in the hands of criminals.

80. Plaintiff Flagella has a continuing interest in ensuring that her Private Information and that of her minor children (all of which remains in the possession of Defendant) is protected and safeguarded from future breaches.

81. As a result of the Data Breach, Plaintiff Flagella made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Flagella has spent several hours dealing with the Data Breach – valuable time she otherwise would have spent on other activities.

82. As a result of the Data Breach, Plaintiff Flagella has suffered anxiety as a result of the release of her minor children's PII, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her minor children's PII for purposes of committing cyber and other crimes against them including, but not limited to, fraud and identity theft. Plaintiff Flagella is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life and the lives of her minor children.

83. Plaintiff Flagella and her minor children also suffered actual injury from having the children's Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her and her children's Private Information, a form of property that Defendant obtained from Plaintiffs; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud they now face.

84. As a result of the Data Breach, Plaintiff Flagella anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

85. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

86. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

87. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

88. As a direct and proximate result of DEF's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

89. Further, as a direct and proximate result of DEF's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

90. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

91. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

92. Plaintiffs and Class Members also lost the benefit of the bargain they made with DEF. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to DEF was intended to be used by DEF to fund adequate security of DEF's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

93. Additionally, as a direct and proximate result of DEF's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

94. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

95. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[13] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[14]

96. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

97. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiffs and Heartland included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiffs and Class Members did not get what they bargained for.

---

[13] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on August 9, 2023).

[14] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 16, 2023).

98. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

99. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of DEF, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

100. As a direct and proximate result of DEF's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

101. Plaintiff brings this action on behalf of herself and her minor children, as well as on behalf of all other persons similarly situated. She does so pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

102. Specifically, Plaintiffs propose the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

103. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

104. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class before the Court determines whether certification is appropriate.

105. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

106. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of roughly 28,539 customers of DEF whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through DEF's records, Class Members' records, publication notice, self-identification, and other means.

107. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether DEF engaged in the conduct alleged herein;

b. When DEF learned of the Data Breach;

c. Whether DEF's response to the Data Breach was adequate;

d. Whether DEF unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether DEF failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether DEF's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether DEF's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether DEF owed a duty to Class Members to safeguard their Private Information;

i. Whether DEF breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether DEF had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether DEF breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether DEF knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of DEF's misconduct;

o. Whether DEF's conduct was negligent;

p. Whether DEF's conduct was *per se* negligent;

q. Whether DEF was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

108. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

109. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

110. Predominance. DEF has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from DEF's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

111. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for DEF. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

112. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). DEF has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

113. Finally, all members of the proposed Class are readily ascertainable. DEF has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by DEF.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class)

114. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

115. DEF knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

116. DEF's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

117. DEF knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. DEF was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

118. DEF owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. DEF's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

119. DEF's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

120. DEF's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

121. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and DEF owed them a duty of care to not subject them to an unreasonable risk of harm.

122. DEF, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within DEF's possession.

123. DEF, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

124. DEF, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

125. DEF breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

126. DEF acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

127. DEF had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust DEF with their Private Information was predicated on the understanding that DEF would take adequate security precautions. Moreover, only DEF had the ability to protect its systems (and the Private Information that it stored on them) from attack.

128. DEF's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated as alleged herein.

129. DEF's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

130. As a result of DEF's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

131. DEF also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

132. As a direct and proximate result of DEF's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

133. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

134. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

135. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring DEF to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class)

136. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

137. Pursuant to Section 5 of the FTCA, DEF had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

138. DEF breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

139. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

140. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of DEF's duty in this regard.

141. DEF violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

142. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to DEF's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

143. DEF's violations of the FTCA constitute negligence *per se*.

144. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to DEF's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

145. As a direct and proximate result of DEF's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

146. DEF breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

147. As a direct and proximate result of DEF's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

148. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring DEF to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

149. Plaintiffs restate and reallege the allegations in stated above as if fully set forth herein.

150. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to DEF in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

151. DEF's Privacy Policy memorialized the rights and obligations of DEF and its customers. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

152. In the Privacy Policy, DEF commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

153. Plaintiffs and Class Members fully performed their obligations under their contracts with DEF.

154. However, DEF did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore DEF breached its contracts with Plaintiffs and Class Members.

155. DEF allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, DEF breached the Privacy Policy with Plaintiffs and Class Members.

156. DEF's failure to satisfy its confidentiality and privacy obligations resulted in DEF providing services to Plaintiffs and Class Members that were of a diminished value.

157. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

158. As a direct and proximate result of DEF's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

159. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring DEF to, *inter alia*, strengthen its data security systems and monitoring

procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

160. Plaintiffs restate and reallege the allegations set forth above as if fully set forth herein.

161. This Count is pleaded in the alternative to Count III above.

162. DEF provides utility assistance services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services from Defendant.

163. Through Defendant's sale of services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with DEF's policies, practices, and applicable law.

164. As consideration, Plaintiffs and Class Members paid money to DEF and turned over valuable Private Information to DEF. Accordingly, Plaintiffs and Class Members bargained with DEF to securely maintain and store their Private Information.

165. DEF accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

166. In delivering their Private Information to DEF and paying for services, Plaintiffs and Class Members intended and understood that DEF would adequately safeguard the Private Information as part of that service.

167. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also

protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

168. Plaintiffs and Class Members would not have entrusted their Private Information to DEF in the absence of such an implied contract.

169. Had DEF disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to DEF.

170. DEF recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

171. DEF violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

172. Plaintiffs and Class Members have been damaged by DEF's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

173. Plaintiffs restate and reallege the allegations set forth above as if fully set forth herein.

174. This Count is pleaded in the alternative to Counts III and IV above.

175. Plaintiffs and Class Members conferred a benefit on DEF by turning over their Private Information to Defendant and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

176. Upon information and belief, DEF funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

177. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to DEF.

178. DEF has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

179. DEF knew that Plaintiffs and Class Members conferred a benefit upon it, which DEF accepted. DEF profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

180. If Plaintiffs and Class Members had known that DEF had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

181. Due to DEF's conduct alleged herein, it would be unjust and inequitable under the circumstances for DEF to be permitted to retain the benefit of its wrongful conduct.

182. As a direct and proximate result of DEF's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in DEF's possession and is subject to further unauthorized disclosures so long as DEF fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

183. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from DEF and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by DEF from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

184. Plaintiffs and Class Members may not have an adequate remedy at law against DEF, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing DEF to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring DEF to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 17, 2023 By: /s/ *Randi Kassan*

Randi Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

Nicholas Sandercock
Mason A. Barney
Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com